

**IN THE UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF NEW YORK**

DIANE AYERDI, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

ZETA GLOBAL HOLDINGS CORP., and
DOTDASH MEREDITH, INC.,

Defendants.

Case No. 1:25-cv-05780

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Diane Ayerdi (“Plaintiff”) files this class action complaint on behalf of herself and all others similarly situated (the “Class Members” and the “Classes”) against Defendants Zeta Global Holdings Corp. (“Defendant,” “Zeta Global,” or “Zeta”) and Dotdash Meredith, Inc. (“Dotdash Meredith” or “Dotdash”). Plaintiff brings this action based upon personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of her counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all California residents who subscribed to an email newsletter that included Zeta’s LiveIntent tracking pixels¹ and click

¹ Pixels—also referred to as tracking pixels, web beacons, or page tags—are 1×1 or similarly sized pixel images embedded in HTML code and used by marketers to monitor and collect information about users’ online activity. In this context, such pixels are employed to track activity specifically related to the reading of email newsletters. Zeta deploys pixels in various areas of websites or newsletters to collect data for the Zeta Marketing Platform, including for purposes of modeling, attribution, and analytics. Zeta Global, Marketing Platform Overview, <https://knowledgebase.zetaglobal.com/gswz/> [<https://web.archive.org/web/2/https://knowledgebase.zetaglobal.com/gswz/>] (last visited June 28, 2025).

trackers² (the “Class” and “Class Members”) and all California residents who were sent such newsletters by Defendant Dotdash Meredith (the “Dotdash Subclass” and “Subclass Members”).

2. Zeta is an identity-data and targeted advertising company that claims to have amassed detailed identity data profiles on approximately 90% of Americans.³ Through the acquisition of at least 23 companies—including numerous so-called “consent farms,”⁴ Zeta has rapidly become the third largest⁵ purveyor of online identity data globally. Zeta leverages its vast trove of data to monitor individuals’ activities and construct comprehensive, cradle-to-grave dossiers containing thousands of unique, privacy-invasive data points. These dossiers are used to deliver targeted advertisements and maximize profits for Zeta’s extensive roster of advertising and publishing clients, which includes 40% of the Fortune 100.

3. Zeta competes with major technology companies like Meta, Google, and Amazon, which are often described as “walled garden” platforms.⁶ Zeta also competes with The Trade Desk, a significant player in the so-called “open internet” advertising sector.⁷ These competitors have

² “Click tracker redirects” are code snippets that track when each clickable element in the email is clicked. This includes headlines, article links, images, social media buttons, footer links, unsubscribe mechanisms, and privacy policy links. The element is wrapped in or replaced with a unique tracking redirect implemented through HTML anchor tags, “<a href>,” which route user clicks through surveillance infrastructure before the link opens.

³ Neej Gore, Chief Data Officer, Zeta Global, Remarks at Zeta Data Summit 2024 (2024), <https://youtu.be/yevfcdml6kM?t=865> at 14:25 (Dec. 9, 2024) (“In the [Zeta] data cloud we see about 90% of the US adult population on a persistent ID basis, meaning we can monitor them across the internet.”).

⁴ A consent farm is a website that coerces consumers into providing their personal information and purportedly agreeing to its sale or disclosure to third parties through misleading promises or confusing consent processes.

⁵ Interview David Steinberg, CEO Zeta Global & Alain Levy, CEO Weborama, Weborama, YouTube (May 18, 2023), at 10:35, <https://youtu.be/-eqcLvQZHTM> (CEO David Steinberg states Zeta holds the “world’s third largest [identity] data set.”).

⁶ A walled garden is a closed online platform where the provider controls content, data, and user access—like Facebook or Google—while the open internet refers to the broader, unrestricted web where users freely access information at “open” websites or applications. Imaginuity, Walled Gardens vs. Open Internet: How Best to Reach Omnichannel Consumers, <https://www.imaginuity.com/blog/walled-gardens-vs-open-internet-how-best-to-reach-omnichannel-consumers/> [<https://web.archive.org/web/2/https://www.imaginuity.com/blog/walled-gardens-vs-open-internet-how-best-to-reach-omnichannel-consumers/>] (last visited June 28, 2025).

⁷ Zeta Global Holdings Corp., Presentation at Morgan Stanley Tech., Media & Telecom Conf. (Mar. 4, 2024), transcript at MarketScreener, <https://www.marketscreener.com/quote/stock/ZETA-GLOBAL-HOLDINGS-CORP-123552310/news/Transcript-Zeta-Global-Holdings-Corp-Presents-at-Morgan-Stanley-s-Technology-Media-Telecom-Con-46101370/> (last visited June 28, 2025); see also *Zeta Global: Reality Hit Very Hard, But the Growth*

faced allegations of serious privacy violations in recent years for conduct similar to, or mirroring, Zeta’s activities. For example, Meta settled *In re Facebook Pixel Tracking Litigation* for \$72 million in 2023.⁸ Google settled *In re Google Real-Time-Bidding Litigation* for \$1.375 billion in May 2025.⁹ The Trade Desk is currently defending several lawsuits relating to its real-time bidding (“RTB”) and dossier-building practices.¹⁰

4. Zeta’s platform launches over two billion cookies¹¹ per month, matching hundreds of millions of these cookies to individuals in its database of consumer identities and identifiers. Zeta collects, merges, and analyzes data from cookies, client CRM systems, call center logs, browsing activity, and other sources, including email newsletter tracking data gathered by its subsidiary LiveIntent (and others), to create unique, persistent profiles of individuals. The Zeta Marketing Platform (“ZMP”) enables clients to attribute marketplace actions like purchases, calls, and complaints to individuals, predict customer behavior, and target or suppress marketing based on detailed behavioral models.

5. Zeta shares, sells, or otherwise discloses personal data and behavioral profiles to its clients and third parties for advertising, marketing, and analytics purposes without first obtaining informed consent of the individuals whose data it collects.

Story’s Not Finished, Seeking Alpha (Mar. 4, 2024), <https://seekingalpha.com/article/4778495-zeta-global-reality-hit-very-hard-growth-story-not-finished> (last visited June 28, 2025).

⁸ Order Granting Final Approval of Class Action Settlement, *In re Facebook, Inc. Consumer Priv. User Profile Litig.*, No. 3:18-md-02843-VC, 2023 WL 7002103 (N.D. Cal. Oct. 10, 2023), <https://angeion-public.s3.amazonaws.com/www.facebookuserprivacysettlement.com/docs/MDL%201182%20ORDER%20GRANTING%20FINAL%20APPROVAL%20101023.pdf> [<https://web.archive.org/web/20240623161054/https://angeion-public.s3.amazonaws.com/www.facebookuserprivacysettlement.com/docs/MDL%201182%20ORDER%20GRANTING%20FINAL%20APPROVAL%20101023.pdf>].

⁹ Consent Judgment, *State v. Google LLC*, No. TX-AG-22-001 (Tex. A.G. May 9, 2025) (imposing \$1.375 billion settlement).

¹⁰ Complaint, *Michie v. The Trade Desk, Inc.*, No. 5:25-cv-01883 (N.D. Cal. Mar. 28, 2025).

¹¹ A “cookie,” as used on websites, is a small text file containing data that a website stores on one’s device via a web browser. This data typically includes a unique identifier and may store information such as the user’s login status, preferences, and past activity.

6. Zeta claims all individuals in its database have “opted in,” but it fails to provide clear, conspicuous notice or obtain meaningful informed consent for the full scope of its data collection, aggregation, and disclosure.

7. Zeta has violated state and federal law by harvesting personal data without consent via client newsletter sign-ups, secretly tracking consumers using its LiveIntent tracking pixel; disclosing personal data to advertisers without informed consent through its LiveIntent real-time bidding process; falsely claiming that it does not sell data; falsely claiming that its consumer data is rendered “privacy-safe” by hashing; matching disparate data sources to create privacy-invasive intent-based signals and sharing such data without informed consent, and using the Zeta ID, LiveIntent ID, and other persistent unique identifiers to build identity dossiers to know and track individuals across all advertising channels and sell, disclose, and redistribute their data to third and fourth parties without informed consent.

8. Plaintiff for herself and all members of the Classes seeks damages and injunctive relief pursuant to the California Invasion of Privacy Act, Cal. Penal Code § 631 (CIPA § 631); the California Invasion of Privacy Act, Cal. Penal Code § 632 (CIPA § 632) the California Consumer Privacy Act, Cal. Civ. Code § 1798.150(a)(1) (CCPA); the California Unfair Competition Law (UCL Bus. & Prof. Code §§ 17200 *et seq.*); violations of the Right to Privacy Under the California Constitution; Intrusion Upon Seclusion under California Common Law; New York General Business Law §§ 349–350; Unjust Enrichment under California and New York Common Law; and seeks Declaratory Judgment.

PARTIES

9. Plaintiff Diane Ayerdi is an adult citizen of the state of California and resides in San Francisco, California. Plaintiff is a subscriber to a newsletter containing the LiveIntent pixel.

10. Defendant Zeta Global is a Delaware corporation with its principal place of business in New York, New York. Zeta provides data-driven “marketing solutions” powered by artificial intelligence. Zeta assists brands in acquiring and retaining customers through personalized advertisements and behavioral targeting.

11. In October 2024, Zeta acquired LiveIntent, Inc., a Delaware corporation headquartered in New York. LiveIntent specializes in email marketing and advertising using real-time bidding, which enables publishers to target specific audiences within newsletters using the LiveIntent tracking pixel. This pixel allows publishers to monetize customer email addresses and other private, personal information. Following the acquisition, Zeta integrated LiveIntent’s technology, publisher network, and consumer identity data into its own marketing platform and assumed responsibility for LiveIntent’s business activities.

12. Defendant Dotdash Meredith, Inc. (“Dotdash Meredith” or “Dotdash”) is a Delaware corporation with its principal place of business at 225 Liberty Street, 4th Floor, New York, NY 10281. Dotdash Meredith also maintains significant operations at 1716 Locust Street, Des Moines, IA 50309. Dotdash Meredith is a leading digital and print publisher, operating well-known brands including People.com.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

14. The Court has general jurisdiction over Defendant because Defendant’s principal place of business is in the State of New York, meaning Defendant is at home in this forum.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this district.

COMMON FACTUAL ALLEGATIONS

16. In 2007, David Steinberg and John Scully, formerly of Apple and Pepsi, co-founded XL Marketing (later known as XLM), which was renamed Zeta Interactive in 2014 and, in 2016, became Zeta Global. Zeta Global is the successor to Steinberg’s first billion-dollar “unicorn,” InPhonic, which was ultimately charged by the Federal Trade Commission with operating an unlawful customer rebate scheme¹² and subsequently filed for bankruptcy.¹³

17. Zeta soon entered a period of rapid growth, acquiring seven or eight companies, including its direct competitor in the United Kingdom, Intela.¹⁴

18. In 2017, Zeta acquired Disqus Inc., a company that provided commenting systems for approximately four million websites. At the time of acquisition, Disqus logged roughly 50 million comments per month and reported reaching two billion unique visitors monthly, generating 17 billion page views. According to Zeta CEO David Steinberg, the acquisition added approximately 1.5 billion additional cookies to Zeta’s already extensive data collection

¹² In 2012, the SEC also charged a former InPhonic executive for “a fraudulent scheme involving a series of ‘round trip transactions to artificially inflate InPhonic’s financial results’ from 2005 to 2007; i.e., during Steinberg’s time as CEO, leading up to the Company’s bankruptcy. The complaint also alleges that the fraud was hidden from auditors. See Litig. Rel. No. 22237, *SEC v. Familant & Greene* (SEC Jan. 25, 2012), <https://www.sec.gov/enforcement-litigation/litigation-releases/lr-22237> [<https://web.archive.org/web/20241116134346/https://www.sec.gov/enforcement-litigation/litigation-releases/lr-22237>]; Complaint, *SEC v. Familant*, No. 1:12-cv-00119 (D.D.C. Jan. 25, 2012), <https://www.sec.gov/files/litigation/complaints/2012/comp22237.pdf> [<https://web.archive.org/web/20241113194920/https://www.sec.gov/files/litigation/complaints/2012/comp22237.pdf>].

¹³ Karsten Strauss, *John Sculley Talks About Mentors, Failure, Reasons To Join A Startup—But Not The Future Of Soda*, Forbes (July 19, 2015), <https://web.archive.org/web/20150723000900/http://www.forbes.com/sites/forbes/treptalks/2015/07/19/john-sculley-talks-about-mentors-failure-reasons-to-join-a-startup-but-not-the-future-of-soda/>.

¹⁴ Anthony Ha, *XL Marketing Buys Adchemy’s Customer Acquisition Division*, TechCrunch (Nov. 4, 2013), <https://techcrunch.com/2013/11/04/xl-marketing-buys-adchemy-actions/> [<https://web.archive.org/web/20250703161722/https://techcrunch.com/2013/11/04/xl-marketing-buys-adchemy-actions/>].

infrastructure. As a direct result of the Disqus acquisition, the number of Zeta's identity profiles increased from approximately 350 million to 600 million within a single year, from 2017 to 2018.¹⁵

19. Zeta made three acquisitions after 2020, also aimed at acquiring consumer identity data to enhance its identity graph. As a result of these acquisitions, Zeta became the third-largest holder of online identity data, amassing more than 1,700 data points for every individual in its database, though in 2019 it claimed up to 2,500 data points per individual.¹⁶

20. Zeta's aggressive acquisition strategy embodied its "One Zeta" philosophy of becoming a centralized platform designed to serve as a one-stop shop for companies seeking to track existing and prospective customers and target them with omni-channel messaging informed by dossier-based intent signals. By acquiring vast quantities of consumer data and identifiers and integrating them into its proprietary identity graph, Zeta directly competes with industry leaders such as Google, Meta, and The Trade Desk. Unlike other marketing technology companies that focus on discrete aspects of digital advertising, Zeta provides both publishers and advertisers with a comprehensive suite of services, including identification, data management, customer management, targeting, outreach, and new customer acquisition. Zeta's market position affords it the unique ability to match, compare, and cross-reference datasets to track millions of consumers both online and offline, aggregating and monetizing trillions of disparate identifier datapoints.

¹⁵ Press Release, *Zeta Global Purchases Disqus for \$90 Million*, NewsCenter.io (Dec. 6, 2017), <https://newscenter.io/2017/12/zeta-global-purchases-disqus-90-million/> [<https://web.archive.org/web/20250709200949/https://newscenter.io/2017/12/zeta-global-purchases-disqus-90-million/>].

¹⁶ Okay, Computer, *Less Cloudy the Ad Future Is: A Conversation with Zeta Global's David Steinberg at 30:00*, Risk Reversal Media (Aug. 24, 2022), <https://podcasts.apple.com/gb/podcast/okay-computer-8-24-22-less-cloudy-the-ad-future-is/id1545205930?i=1000577185119> ("[W]e're building a consumer data platform or CDP. Our client's data goes into it. We match usually around 85% of the data to our US-based data cloud, which is 235 million opted-in Americans, and we import an average of 1700 data elements per person. We then remove their name, we remove their social security number, and we replace it with Zeta ID 13578."); George P. Slefo, *Zeta Acquires DSP from Sizmek, Takes Aim at The Trade Desk*, Ad Age (Apr. 19, 2019), <https://web.archive.org/web/20231207093746/https://adage.com/article/digital/zeta-acquires-dsp-sizmek-takes-aim-trade-desk/2165707> (CEO David Steinberg: "We have 2,500 data points on each person in our database, with 240 million active Americans in the U.S. today.").

Zeta Acquires LiveIntent

21. On October 8, 2024, Zeta announced that it had entered into an agreement to acquire LiveIntent to enhance Zeta's identity resolution capabilities.

22. With its acquisition of LiveIntent, Zeta added to its network over 2,000 premium publishers, including eight of the top 10 largest publishers in the Comscore rankings.

23. LiveIntent operates an email pixel tracking service embedded in marketing emails and newsletters.

24. When a consumer subscribes to a newsletter distributed by a LiveIntent publisher, LiveIntent embeds a pixel within the email. When the consumer opens the email, the pixel is triggered, resulting in the collection and transmission of the consumer's IP address and email address to Zeta.

25. LiveIntent contributes 235 million unique hashed email addresses per month to Zeta's identity graph, which allows Zeta to track and engage users across different devices and platforms, infer intent signals, and resell such data to other Zeta customers.

Defendant Dotdash Meredith Intercepts and Retransmits the Class Members' Personal Information to Zeta Without Informed Consent Using the LiveIntent Pixel Tracker

26. Dotdash implements the LiveIntent pixel in its People.com newsletters and other email communications, allowing for the collection of user engagement data. Dotdash transmits data collected via the pixel—including hashed email addresses, and in some instances, plaintext email addresses, and behavioral information—directly to LiveIntent and, by extension, Zeta Global, which has acquired LiveIntent and its database of over 235 million unique email addresses, including those from Dotdash Meredith's audience.

27. Dotdash thereby enables third and fourth-party tracking and targeting, as LiveIntent and Zeta Global use the transmitted data to build extensive user profiles and dossiers and facilitate targeted advertising at scale across their combined publisher and advertiser networks.

28. Dotdash fails to obtain informed consent from newsletter subscribers prior to the collection and sharing of this personal and behavioral information. Dotdash Meredith does not provide clear, conspicuous notice or a meaningful opportunity for subscribers to consent to or opt out of such tracking and data sharing before it occurs.

29. As a result, Dotdash Meredith's practices allow for the unconsented tracking of newsletter subscribers and the dissemination of their personal data to third parties for advertising and profiling purposes, in violation of consumer privacy rights and applicable law.

30. When consumers like Plaintiff Ayerdi open an email newsletter containing the LiveIntent tracking pixel, LiveIntent runs ad auctions to determine which ads it will display.

31. Dotdash Meredith embeds the LiveIntent pixel in its email newsletters distributed to subscribers of People.com and other properties. The LiveIntent pixel is a tracking technology that enables the collection of data about newsletter recipients' interactions, including when and where the email is opened, device information, and subsequent online activity. This data is then transmitted to LiveIntent, and, following LiveIntent's acquisition, to Zeta Global Holdings Corp.

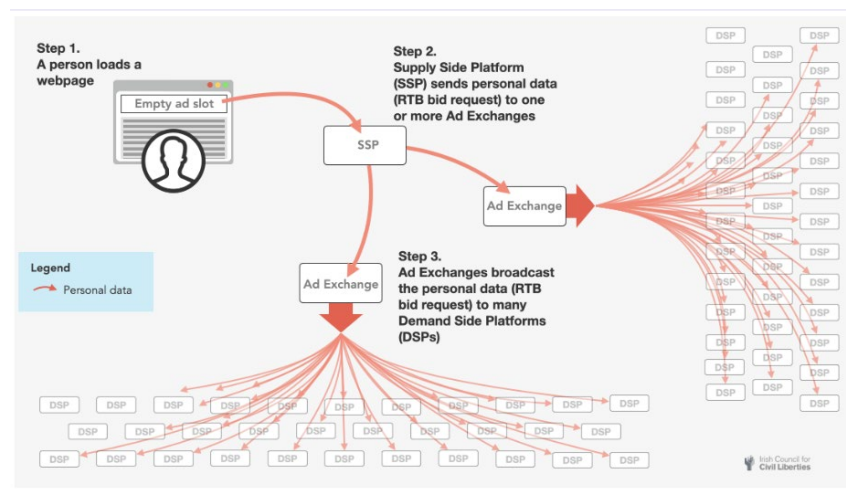
Zeta Shares Personal Information Through LiveIntent's Real-Time Bidding Platform

32. The LiveIntent pixel allows Zeta to track user behavior and deliver targeted advertisements to the consumer through a process called real-time bidding or RTB.

33. RTB functions such that, when an email client loads an image, the resulting impression is auctioned to the highest bidder in milliseconds. This process occurs in real time and

involves multiple demand side platform (“DSP”) ¹⁷ partners, including Google’s Invite (Bid Manager), MediaMath, DataLogix, and TapAd, along with Zeta’s own DSP.

34. Publishers monetize their customer databases—including names and email addresses—by integrating LiveIntent’s tracking pixel into their email newsletters, thereby enabling targeted advertising and data-driven marketing campaigns. Advertisers use LiveIntent’s exchange to bid on email inventory and target individual consumers based on specific targeting criteria. By way of illustration:



35. LiveIntent operates its own RTB exchange, LiveIntent Exchange, where email impressions are auctioned to advertisers. Zeta Marketing Platform (ZMP) is unique in the industry because it offers both a Supply Side Platform and a Demand Side Platform. Zeta CEO David Steinberg reports that Zeta “is the only platform that merges the data cloud and the marketing cloud into one ecosystem.”¹⁸

¹⁷ A demand-side platform (“DSP”) is an advertising technology platform that advertisers and agencies use to buy digital advertising inventory across multiple ad exchanges and supply-side platforms in real-time. Wikipedia, Demand-Side Platform, https://en.wikipedia.org/wiki/Demand-side_platform [https://web.archive.org/web/2/https://en.wikipedia.org/wiki/Demand-side_platform] (last visited June 28, 2025).

¹⁸ David Steinberg, Interview on MarTech Podcast, Episode 256 at 10:00 (Dec. 30, 2019), <https://podcasts.apple.com/gb/podcast/launching-scaling-a-martech-unicorn-david-steinberg/id1360406217?i=1000461115150>.

36. Like all RTB exchanges, once there is a request from the email user triggered by opening the email, the impression is offered to bidders in the RTB auction.¹⁹

37. The process starts with an email newsletter publisher, like People, sending information about the user and content to Zeta, which ingests it into its identity graph, and subsequently shares that data with other Zeta customers.²⁰

38. Zeta then packages all the information it can gather about the individual into a “bid request” and broadcasts it to thousands of potential advertisers. The bid request may contain personal information like unique advertising ID, location, IP address, device details, interests, and demographic information. The information in bid requests is called “bidstream data” and its traders can attribute it to individuals through profiling.

39. Advertisers utilize the personal information contained in each bid request to determine whether to bid on available ad space. Zeta’s customers profile, target, and track individuals using Zeta’s various services.

40. A fundamental vulnerability of RTB is that, although only one advertiser ultimately wins the auction, all participating bidders receive the data associated with each auction. As a result, any entity purporting to act as an ad buyer can access a continuous stream of sensitive information concerning billions of individuals who use websites or mobile applications that serve targeted advertisements. RTB thereby transmits personal data to data brokers, who, in turn, sell this information to any purchaser willing to pay.

¹⁹ Allison Schiff, *Growing the Email Display Ad Exchange at LiveIntent*, AdExchanger (Aug. 9, 2019), <https://www.adexchanger.com/email/email-display-ad-exchange-liveintent/> [https://web.archive.org/web/20241003-200946/https://www.adexchanger.com/email/email-display-ad-exchange-liveintent/].

²⁰ Matt Prohaska, *Unlike Other Marketing Clouds, Zeta Global Is Betting on Its DSP*, AdExchanger (Mar. 16, 2020), <https://www.adexchanger.com/online-advertising/unlike-other-marketing-clouds-zeta-global-is-betting-on-its-dsp-can-it-pay-off/> [https://web.archive.org/web/20241003200946/https://www.adexchanger.com/email/email-display-ad-exchange-liveintent/] (last visited June 28, 2025).

41. Data brokers actively rely on RTB to collect and sell sensitive information. For example, the Federal Trade Commission (“FTC”) found that data broker Mobilewalla was collecting personal data—including precise location information—from RTB auctions without placing ads. Mobilewalla collected data on over a billion people, with an estimated 60% sourced directly from RTB auctions.²¹ The company then sold this data for a range of invasive purposes, including tracking union organizers, tracking people at Black Lives Matter protests, and compiling home addresses of healthcare employees for recruitment by competing employers. It also categorized people into custom groups for advertisers, such as “pregnant women,” “Hispanic churchgoers,” and “members of the LGBTQ+ community.”²² The FTC concluded that Mobilewalla’s practice of collecting personal data from RTB auctions without placing ads violated the FTC Act’s prohibition of unfair conduct.²³

42. Zeta’s services are based on its ability to collect and analyze consumer behavior online and offline and deliver that data to its Publisher and Advertiser clients, who use that data for targeted advertising and monetization.

43. Zeta combines its disparate identity data sources, including those harvested from Disqus websites and others, to inform LiveIntent publisher and advertiser customers how to identify, profile, target, and track individuals and infer their future intents.

²¹ Decision & Order, *In re Mobilewalla, Inc.*, FTC File No. 2023196 (Dec. 6, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallaorder.pdf [https://web.archive.org/web/20250409-022810/https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallaorder.pdf] (last visited June 28, 2025).

²² Complaint ¶ 45, *FTC v. Mobilewalla Inc.*, FTC File No. 2023196 (Dec. 6, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallaacco.pdf [https://web.archive.org/web/20250409-022810/https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallaacco.pdf].

²³ Stipulated Order for Permanent Injunction § III(D), *FTC v. Mobilewalla Inc.*, FTC File No. 2023196 (Dec. 6, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallaacco.pdf [https://web.archive.org/web/20250409-022810/https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallaacco.pdf].

44. All identifiers and signals, including intent signals collected by Zeta, constitute personal information because they “divulge a user’s personal interests, queries, and habits.” *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 605 (9th Cir. 2020).

Zeta Did Not Receive Informed Consent to Intercept, Use, or Disclose Plaintiff’s and the Class Members’ Personal Data

45. Zeta did not disclose to Plaintiff or any Class Member the extent to which it tracks their online and offline activity, builds identity dossiers, and infers their future intent from such data.

46. A reasonable consumer would not expect that merely opening an email newsletter containing ads powered by LiveIntent and Zeta would result in LiveIntent and Zeta tracking their activities across the entire “open web,” as well as monitoring their offline activities.

47. Zeta does not disclose to their LiveIntent-powered newsletter readers that their newsletter reading activities are being monitored by the LiveIntent tracking pixel. This lack of information prevents consumers like Plaintiff and the Class Members from contacting Zeta to request deletion of their PII.

48. Zeta claims that 245 million “US Individuals [are] Eligible for Online Tracking via Acceptance of Zeta Publisher Terms of Service.”²⁴

49. Plaintiff is unaware of and has not ever seen Zeta’s “Publisher Terms of Service.”

²⁴ Zeta Global, Investor Presentation slide 38 (2025), https://investors.zetaglobal.com/events-and-presentations/presentations/default.aspx?gl=1*1ej729g*_gcl_au*MTMzNzE0MDIyMy4xNzQ2ODExNTE2*_ga*MTQ1MzM2NjYwMi4xNzQ2ODExNTE2*_ga_H1DTS3V7ZB*cze3NDczNTE1MTYkbzEwJGcwJHJHxNzQ3MzUxNTE2JGo2MCRsMCRoMTcyNTE5ODgyNw [https://web.archive.org/web/20250703163729/https://s202.q4cdn.com/623583957/files/doc_financials/2025/q1/ZE-TA-1Q-25-Earnings-Supplemental.pdf] (last visited June 28, 2025).

50. Zeta does not require opt-in consent for cookies and places the responsibility for notice and opt-out mechanisms on publishers.²⁵

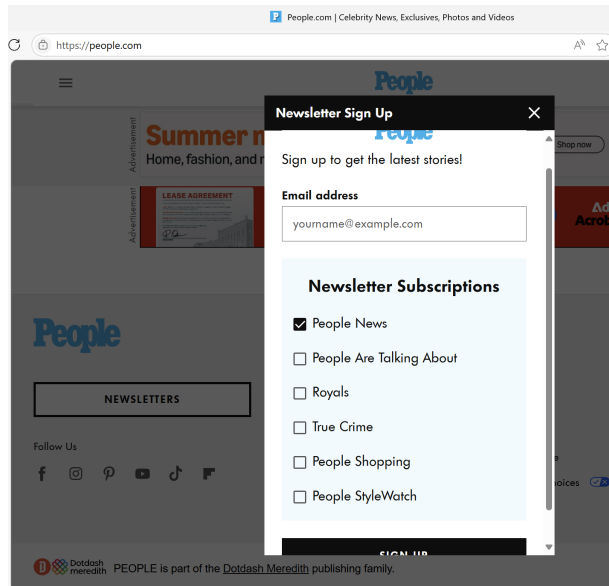
Zeta Sent the LiveIntent Pixel to Plaintiff and Deployed it Without Consent

51. On or about June 25, 2025, while in California, Plaintiff Ayerdi visited a website operated by Zeta’s client, Dotdash Meredith, at <https://people.com>. While on the website, Plaintiff subscribed to a newsletter offered by People, one of Dotdash Meredith’s brands, by submitting her email address in a webform. Plaintiff then received an email newsletter from People and Dotdash Meredith containing Zeta’s LiveIntent tracking pixel.

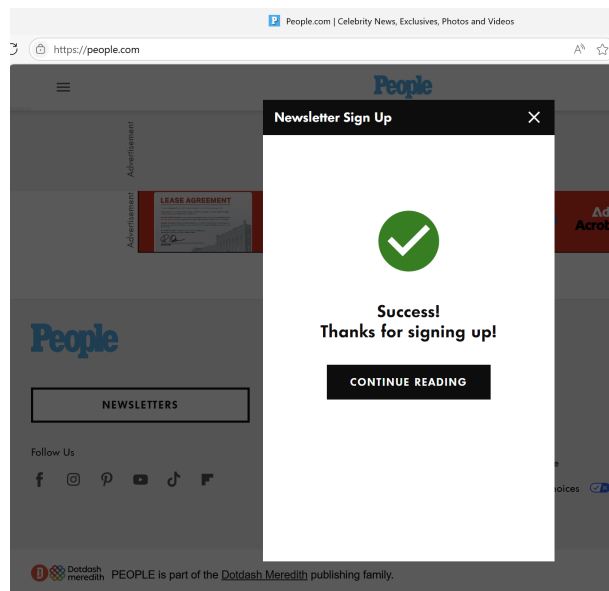
52. Upon opening the email newsletter, Zeta tracked Plaintiff’s online activities and associated this behavioral data with its identity graph, compiling detailed inferences regarding Plaintiff’s activities, habits, propensities, and intents. Zeta then monetized these inferences by offering them for sale to third-party customers through its platform.

53. The Newsletter Sign Up webform presented to Plaintiff, pictured below, did not require Plaintiff to “opt in” to the use of the LiveIntent pixel. In fact, the webform did not include any hyperlink at all. The webform did not present a hyperlink to any terms of service or any privacy policy:

²⁵ Zeta Global, *Data Privacy Overview*, <https://knowledgebase.zetaglobal.com/kb/data-privacy> [https://web.archive.org/web/20250703163643/https://investors.zetaglobal.com/events-and-presentations/presentations/default.aspx?gl=1%2A1ej729g%2A_gcl_au%2AMTMzNzE0MDIyMy4xNzQ2ODExNTE2%2A_ga%2AMTQ1MzM2NjYwMi4xNzQ2ODExNTE2%2A_ga_H1DTS3V7ZB%2AczE3NDczNTE1MTYk bzEwJGcwJHQxNzQ3MzUxNTE2JGo2MCRsMCRoMTcyNTE5ODgyNw] (“Zeta does not require opt-in consent for cookies and places the responsibility for notice and opt-out mechanisms on publishers”) (last visited June 28, 2025).

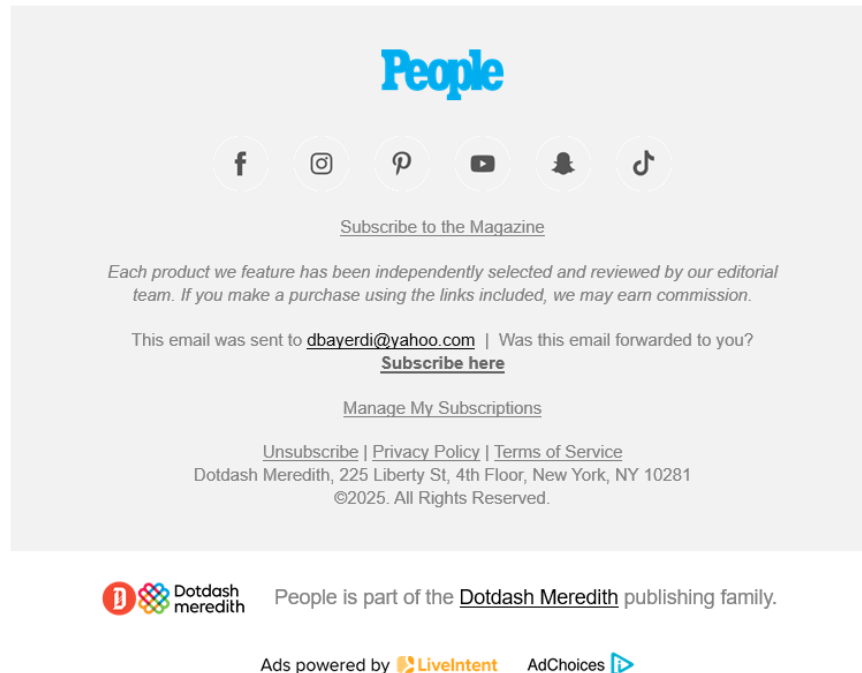


54. After Plaintiff entered her email address by typing it in the “Email address” field and clicking “SIGN UP,” the following screen appeared. Once again, there was no hyperlink to terms of service or privacy policy.



55. Next, Plaintiff received an email from People. This email contained the LiveIntent tracker and served a targeted advertisement to Plaintiff.

56. The bottom of the email newsletter from People showed the following:



57. As seen, the email includes hyperlinks to Dotdash Meredith’s Privacy Policy and Terms of Service; however, Plaintiff was not required to click on those hyperlinks, read them, or assent to the Terms of Service or Privacy Policy before reading the newsletter, interacting with it, and having her data intercepted by Zeta.

58. Zeta intercepts individuals’ confidential communications without obtaining their informed consent.

59. Zeta does not inform newsletter subscribers that it intercepts their communications with its publisher partners.

60. Zeta and its publisher clients do not get informed consent from website users or newsletter subscribers.

Forty Three Trackers in the People.com Email Newsletter to Plaintiff

61. Attached as Exhibit A is a PDF printout of the email newsletter received by Plaintiff Ayerdi from People.com on June 25 2025 (“People.com Newsletter”). Attached as Exhibit B is the email when viewed as HTML code showing the ***forty-three (43) trackers*** described below.

62. The June 25 2025 People.com newsletter embedded 13 covert tracking pixels—2 operated by People.com and 11 operated by LiveIntent / Zeta Global (including 5 “SAFE RTB” auction beacons). Each pixel automatically transmitted Plaintiff’s email address, IP address, device fingerprint, and open-time metadata to third-party servers the moment the email is opened, without any notice or consent.

63. In addition to the 13 covert tracking pixels, the newsletter embedded thirty (30) distinct click-tracking mechanisms, “click trackers.”²⁶ Each clickable element in the email—including but not limited to headlines, article links, images, social media buttons, footer links, unsubscribe mechanisms, and privacy policy links—was wrapped in or replaced with a unique tracking redirect implemented through HTML anchor tags (<a href>) that route user clicks through surveillance infrastructure before reaching the intended destination.

64. These click-tracking mechanisms operate through HTML anchor tag (<a href>) manipulation, where each legitimate destination URL is replaced with a tracking redirect URL following the pattern [https://links.people.com/u/click?\[tracking_parameters\]](https://links.people.com/u/click?[tracking_parameters]) or [https://links.people.com/e/eh?\[tracking_parameters\]](https://links.people.com/e/eh?[tracking_parameters]). When any tracked element is clicked, the user's browser is first redirected to People.com's tracking servers, which log the click event along with the recipient's email address, timestamp, specific element clicked, device information, and referrer data, before forwarding the user to the intended destination.

	Tracker Type and Function	No.
1	Two (2) People.com pixels: Confirm email open, log IP address, and timestamp for the sender.	2
2	Six (6) LiveIntent pixels: Transmit your email address, device type, and behavioral data to LiveIntent (now Zeta Global) for profiling and cross-device tracking.	6

²⁶ Click trackers are also known as URL beacons, link beacons, redirect beacons, click interceptors, bounce trackers, navigation trackers, link wrappers, tracking anchors, hyperlink trackers, interaction monitors, engagement trackers, click surveillance mechanisms, link monitoring systems, click monitoring apparatus, and redirect-based data collection systems.

	Tracker Type and Function	No.
3	Five (5) “SAFE RTB” pixels: Send your data to real-time ad auctions, exposing it to hundreds of potential bidders.	5
4	Thirty (30) Click tracker redirects (aka URL beacons, redirect beacons, and <a href> redirects): Log every click you make in the email, including on images, headlines, social media, and even privacy-related links.	30
	Total	43

Five Safe RTB Pixels (5)

65. The LiveIntent RTB tracking section is marked by the phrase

“<!-- SAFE RTB -->.” It follows with:

```
<table cellpadding="0" cellspacing="0" border="0" width="40" height="6">
  <tbody>
    <tr>
      <td>
        
      </td>
      <td>
        
      </td>
      <td>
        
      </td>
      <td>
        
      </td>
      <td>
        
      </td>
    </tr>
  </tbody>
</table>
```

66. Each “” tag in this section is a tracking pixel, differing only by the incrementing value of the “s” parameter. Each RTB pixel URL contains several query parameters:

Parameter	Value	Use
s	125532100–125532104	Unique RTB segment/impression ID
li	PPL_BreakingNews	Campaign/newsletter identifier
e	<u>dbayerdi@yahoo.com</u>	Recipient's email address
p	20250625	Send date or campaign ID
lctg	c273891e71ab67b...	Campaign tracking code/hash
stpe	pixel	Pixel type (RTB tracking)
IP/User Agent	(from HTTP request)	Device, location, and client identification

67. When the email is opened, the recipient's email client automatically requests each of these images from LiveIntent's server. This request transmits all the above parameters, along with the recipient's IP address and user agent (browser or device information), which are included in every HTTP request. All five RTB pixels are loaded as soon as the email is opened, and each pixel request sends the full set of parameters to LiveIntent's servers, including the recipient's email address, campaign, and unique identifiers.

68. LiveIntent receives these requests and uses them to log the open event and all associated metadata, initiate real-time bid requests to advertising partners using the recipient's data for targeting, and record which pixels were loaded, when, and from what device or IP address. The RTB pixels thus collect data for real-time audience segmentation, cross-device and cross-campaign user identification, and feed behavioral data into broader advertising and targeting systems.

69. Using five sequential pixels, each with a unique "s" value, creates redundancy (ensuring at least one pixel loads even if others are blocked), multiple bid opportunities (each pixel can represent a separate ad slot or auction event), and enhanced measurement (tracking partial loads or client-specific behaviors).

70. The People.com email newsletter embeds a set of invisible, sequential tracking pixels to transmit detailed, user-specific data to LiveIntent. This enables real-time advertising auctions and persistent user profiling. The data collected includes Plaintiff Ayerdi's email address, campaign identifiers, Plaintiff Ayerdi's device and client information, and unique impression IDs.

Zeta Added Plaintiff's Data to Her Unique Zeta Identity Data Dossier

71. Including Plaintiff Ayerdi's email address in the pixel URL allows LiveIntent, Zeta Global, and their advertising and publishing partners to tie email engagement directly to a persistent, real-world identity, which is highly valuable for ad targeting and measurement. When the email is opened, the recipient's email address is transmitted in plain text to LiveIntent, enabling direct identification. Each open event is logged with device details, IP address, and campaign context, allowing for detailed behavioral profiling. LiveIntent, as an ad exchange, shares or sells this data to other advertisers, data brokers, or partners for further targeting and analytics.

72. This tracking was completely invisible to Plaintiff Ayerdi, as the pixels are too small to be seen and are not disclosed anywhere in the visible content of the email. Plaintiff Ayerdi did not consent to this data sharing and had no knowledge that its existence was being used by Zeta Global to gather her personal information into a data dossier containing an average of 1,700 to 2,500 unique data points for resharing and resale to third and fourth parties.

Zeta's Non-Consensual Data Collection, Use, and Monetization Harms Consumers

73. Zeta's data collection practices involve extensive tracking of consumers across various contexts, including online browsing, mobile usage, and offline activities. This cross-context behavioral advertising allows Zeta to build detailed profiles of individuals, which includes sensitive personal information inferred from their behavior and interactions.

74. Zeta segments consumers into categories based on sensitive information, such as health conditions, religious beliefs, and political affiliations. This information is inferred from users' online behavior and interactions, leading to highly targeted and potentially discriminatory advertising practices.

75. Through re-identification, Zeta assembles pseudonymized data to identify individuals and allow it to create detailed and intrusive profiles of individuals, which are used for highly targeted advertising.

76. In this instance, Zeta captured and tracked granular detail of all Plaintiff's interactions on the newsletter through screen viewing actions to infer time spent reading sections and links clicked.

77. Zeta used its recordings of Plaintiff's interactions on the newsletter email from People.com to infer her interests based on reading activity.

78. Zeta packaged and reshared those inferences for audience building to third party advertisers in exchange for payment through RTB auctions.

79. Zeta stored or determined whether they needed to store those inferences to Plaintiff's unique identity data profile—her Zeta dossier containing 1700–2500 data points—to the extent they were not already in her data profile.

80. Defendants' have done the same to millions of Californians and persons throughout the United States who subscribe to newsletters containing their tracking pixels.

81. When signing up for a newsletter, Plaintiff and the Class Members only consented to receive a newsletter. They did not consent to having their activities while reading the newsletter tracked and did not consent to having their newsletter activities added to Zeta's identity dossier for further resale.

Zeta's Tracking Pixels Constitute Illegal Pen Registers

82. Each of the tracking pixels deployed by LiveIntent and Zeta Global in the newsletters distributed by Dotdash Meredith and People.com constitute "pen registers" under

California Penal Code § 638.51. The pixels recorded addressing and routing information, including IP addresses and email addresses transmitted from Plaintiff's device.

83. When subscribing to the People.com newsletter, Plaintiff Ayerdi and the Class Members were not required to review or affirmatively consent to any privacy policy or terms of service by any Defendant. Plaintiff did not give her informed consent to allow Defendants to store, aggregate, or profile her personal data. Likewise, when LiveIntent used its pixel trackers to transmit Plaintiff's IP addresses, email addresses, and other identifying information each time a newsletter was opened, this collection and transmission occurred without Plaintiff's knowledge or express consent.

84. Any purported consent obtained by People.com is not valid as to LiveIntent or Zeta Global.

85. The conduct of Zeta Global and Dotdash Meredith is not justified by any court order or statutory exception. At no time did Defendants obtain a court order authorizing the installation or use of a pen register or similar device on Plaintiff's communications.

86. Plaintiff and the Class Members are unaware of the presence or operation of these tracking pixels. The terms governing their use are not reasonably conspicuous, and any links to such terms are buried or obscured, failing to provide adequate notice or opportunity for meaningfully informed consent under applicable law(s).

87. Without informed consent, Zeta Global uses newsletter subscriptions as its justification and alleged permission to track a large portion of 90% of Americans both online and offline and create dossiers containing the most intimate details of their lives, compiling 1700 to 2500 data points on each person for resharing and resale to 40% of the Fortune 100 companies for tracking and marketing purposes, in violation of state and federal privacy laws.

Zeta's Inference-Selling Is Highly Offensive and Objectionable to the Reasonable Person

88. Without informed consent, Zeta's processing of such personal, sensitive data with machine learning algorithms and artificial intelligence to infer Class Members' future purchasing intents, peculiarities, or proclivities, and the subsequent publishing of those intents and inferences to, *inter alia*, 40% of the Fortune 100 companies is highly offensive and/or objectionable to the reasonable person.

89. *Zeta's technology stack effectively allows for it to know when a consumer will or will not purchase something before the consumer itself is aware of that intent.* Its clients are then able to capitalize on such knowledge and "nudge" the consumer towards a purchase.

90. Resale and application of such inferences thoroughly highly targeted, personalized, time-specific, and channel-specific marketing based on inferences of future intents is particularly offensive and objectionable because it negates legitimate consumer choice and creates a stark power imbalance in favor of brands and advertisers.

CLASS ALLEGATIONS

91. Plaintiff Ayerdi brings this action individually and on behalf of all others similarly situated (the "Class" or "Class Members") defined as follows: "All residents of California who opened an email newsletter containing the LiveIntent pixel during the relevant statute of limitations period."

92. In addition, Plaintiff Ayerdi brings this action individually and on behalf of all others similarly situated ("Dotdash Subclass" and "Subclass Members") defined as follows: "All residents of California who opened an email newsletter from Dotdash Meredith containing the LiveIntent pixel during the relevant statute of limitations period."

93. The "Class" and the "Dotdash Subclass" together are referred to as the "Classes."

94. Excluded from the Classes are: (i) Defendants, including any affiliate, parent, or subsidiary of Defendants, any entity in which Defendants have a controlling interest, any officer director, or employee of Defendants, and any successor or assign of Defendants; (ii) anyone employed by counsel in this action; and (iii) any judge to whom this case is assigned, his or her spouse and immediate family members, or members of the judge's staff.

95. **Numerosity.** Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time; however, it is estimated that there are many millions of individuals in the Classes. Class Members can be readily identified from Zeta's records.

96. **Typicality.** Plaintiff's claims are typical of the claims of the Classes because Plaintiff, like all other members, viewed a newsletter powered by LiveIntent and had her confidential electronic communications intercepted and disclosed to third parties.

97. **Adequacy.** Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Classes. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

98. **Common Questions of Law and Fact Predominate.** Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members of the Classes because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Class include, but are not limited to, the following:

- whether Zeta installed, executed or embedded the LiveIntent tracking pixel in its publishers' email newsletters;
- whether Zeta obtained consent to collect and share Plaintiff's and Class Members' personal information;
- whether Zeta violated CIPA;
- whether Zeta violated CPPA;
- whether Plaintiff and Class Members are entitled to statutory penalties; and
- whether Class Members are entitled to injunctive relief.

Questions of law and fact common to the Dotdash Subclass include, but are not limited to, the following:

- whether Dotdash sent Plaintiff and the Subclass Members emails containing the LiveIntent tracking pixel;
- whether the tracking pixel sent by Dotdash collected the Subclass Members' personal data;
- whether such data was sent by Dotdash to LiveIntent and Zeta Global; and
- whether Dotdash obtained the Subclass Members' informed consent prior to collecting and sharing their personal data.

99. **Superiority.** Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not

practicably be pursued individually, substantially outweigh potential difficulties in the management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

COUNT I

Violation of California Invasion of Privacy Act (CIPA) – Pen Register Statute (Cal. Penal Code § 638.51) On Behalf of Plaintiff and All Class Members

100. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

101. Defendants, without the knowledge or consent of Plaintiff, installed and used “pen registers” as defined by Cal. Penal Code § 638.50(b) by deploying tracking pixels in newsletters sent to Plaintiff and Class Members.

102. Defendants did not obtain a court order authorizing the installation or use of such a device or process.

103. Defendants’ conduct was not subject to any statutory exception or defense.

104. As a direct and proximate result of Defendants’ actions, Plaintiff and Class Members suffered an invasion of their privacy and the unauthorized collection of their personal information.

105. Plaintiff and Class Members are entitled to statutory damages, injunctive relief, and any other relief deemed appropriate by the Court.

COUNT II

Violation of California Invasion of Privacy Act (CIPA) – Lack of Consent (Cal. Penal Code § 638.51) On Behalf of Plaintiff and All Class Members

106. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

107. Defendants failed to obtain clear, express, and affirmative consent from Plaintiff prior to collecting, storing, and aggregating Plaintiff's personal information through the use of click trackers and tracking pixels.

108. Any purported consent obtained by Dotdash Meredith and People.com was insufficient, as it does not specifically authorize LiveIntent or Zeta Global to collect or process Plaintiff's data.

109. Defendants' use of browsewrap or otherwise inconspicuous agreements does not constitute valid consent under California law.

110. As a result of Defendants' failure to obtain proper consent, Plaintiff and Class Members have suffered harm, including the loss of control over their personal information and the invasion of their privacy.

111. Plaintiff and Class Members seek statutory damages, injunctive relief, and any other relief the Court deems just and proper.

COUNT III

Violation of California Invasion of Privacy Act, Cal. Penal Code § 631 (CIPA § 631) On Behalf of Plaintiff and All Class Members

112. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

113. CIPA § 631(a) prohibits any person who uses a "machine, instrument, contrivance" or "in any other manner" who (1) intentionally taps, or makes any unauthorized connection, with "any telegraph or telephone wire, line, cable, or instrument"; (2) willfully and without the consent of "all parties to the communication" or "in any unauthorized manner," reads or "attempts to read" or "learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within"

California; (3) “uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way” information so obtained; or (4) aids, agrees with, employs, or conspires with “any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.”

114. Zeta’s LiveIntent tracking pixels are each a “machine, instrument, contrivance, or . . . other manner” used to engage in the prohibited conduct at issue here.

115. Zeta’s email pixel tracking devices are implemented by separate legal entities that offer “software-as-a-service” (newsletter “Publishers”) and are not merely passive devices.

116. Zeta had the capability to use the wiretapped information for its own purposes. Accordingly, Zeta was a third party to any communication between Plaintiff and Class Members, on the one hand, and the newsletter Publisher, on the other.

117. At all relevant times, Zeta willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and Class Members, on the one hand, and newsletter Publishers, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

118. At all relevant times, Zeta intentionally used its LiveIntent tracking pixels to eavesdrop upon and record such confidential communications, including, *inter alia*, the location of Plaintiff and the Class Members, which constitutes confidential information within the meaning of CIPA.

119. At all relevant times, Zeta used or attempted to use the communications intercepted by LiveIntent’s tracking pixels to identify, profile, target, and track individuals and infer their future intents, and for resale of such collected and inferred data.

120. Plaintiff and Class Members did not provide their prior consent for Zeta's intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff's and Class Members' electronic communications.

121. The wiretapping of Plaintiff and Class Members occurred in California, where Plaintiff and Class Members accessed the Publishers' email newsletters, and in New York, where Zeta routed Plaintiff's and Class Members' intercepted electronic communications to their data servers.

122. Using the LiveIntent pixels embedded in email newsletters, Zeta agreed with, employed, and conspired with its Publisher clients to tap, intercept, read, and communicate to third parties, including its advertiser clients ("Advertisers") and downstream RTB auction participants, Plaintiff's and the Class Members' communications with Zeta's Publisher clients, including communications that were sent using the LiveIntent pixels without the Class Members' knowledge

123. Through its RTB auctions, Zeta further disclosed and monetized consumer data without informed consent to numerous additional downstream RTB auction bidders.

124. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendants' violations of CIPA § 631(a), and each seeks statutory damages of \$5,000 for each of Defendants' violations of CIPA § 631(a).

COUNT IV

Violation of the California Invasion of Privacy Act, Cal. Penal Code § 632 (CIPA § 632) On Behalf of Plaintiff and All Class Members

125. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

126. CIPA § 632(a) prohibits entities from:

intentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

127. Zeta's LiveIntent tracking pixels deployed on individual newsletters in each instance constitute an electronic amplifying or recording device.

128. At all relevant times, the communications between Plaintiff and Class Members on one hand, and the Publishers on the other, were confidential.

129. At all relevant times, Zeta intentionally used its LiveIntent tracking pixels to eavesdrop upon and record such confidential communications, including, inter alia, the location of Plaintiff and the Class Members, which constitutes confidential information within the meaning of CIPA.

130. When communicating with the Publishers, Plaintiff and Class Members had an objectively reasonable expectation of privacy. Plaintiff and Class Members did not reasonably expect the Publishers to collect any additional information from their newsletter-reading aside from their email addresses, or expect anyone other than the Publishers to be a party to the communications, and did not expect that other, third-party entities, like Zeta, would intentionally use an electronic amplifying or recording device to eavesdrop upon and record their confidential communications.

131. Through its RTB auctions, Defendant further monetized and disclosed consumer data to its Advertiser clients and downstream RTB auction participants without informed consent.

132. Plaintiff and Class Members did not consent to Zeta's actions. Nor have Plaintiff and Class Members consented to Zeta's intentional use of an electronic amplifying or recording

device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

133. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendants' violations of CIPA § 632(a), and each seeks statutory damages of \$5,000 for each of Defendants' violations of CIPA § 632(a).

COUNT V

Violation of California Consumer Privacy Act, Cal. Civ. Code § 1798.150(a)(1) (CCPA) On Behalf of Plaintiff and All Class Members

134. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

135. Plaintiff and the Class Members are consumers whose plaintext, nonencrypted and nonredacted personal information was subject to an unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty to implement and maintain reasonable security practices.

136. Defendant failed to ensure Plaintiff and the Class Members received explicit notice and were provided an opportunity to exercise the right to opt-out of their data collection, use, and sharing practices.

137. Defendant knowingly collected, used, and sold Plaintiff's personal information to third and fourth parties without her consent by embedding the LiveIntent tracking pixel in Publisher newsletters sent to Plaintiff.

138. Defendant then further disclosed and amplified the contents of the communications between Plaintiff and the Publishers to its Advertiser clients and further downstream RTB auction participants.

139. Pursuant to Ca. Civ. Code § 1798.150(b), Plaintiff will send Defendant notice of her CCPA claim shortly after the date of this filing. If Defendant does not correct its business

practices, Plaintiff will amend (or seek leave to amend) the complaint to add claims for monetary relief, including statutory and actual damages under the CCPA. To date, Defendant has failed to cure the CCPA violation.

140. As a result of Defendant's reckless violations, Plaintiff is entitled to actual damages, statutory damages, and attorneys' fees and costs. Ca. Civ. Code § 1798.150.

COUNT VI

Violation of California Unfair Competition Law (Bus. & Prof. Code §§ 17200 *et seq.*) (UCL) On Behalf of Plaintiff and All Class Members

141. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

142. Defendant engaged in unlawful and unfair business practices by collecting, storing, and selling, sharing, or disclosing Plaintiff's personal data without adequate notice or informed consent.

143. Defendant engaged in unlawful business practices by deploying the LiveIntent tracking pixel, disclosing data through RTB auctions, intent signal creation, and dossier-building and data disclosure, distribution, and resale.

144. Defendant deceived consumers by falsely claiming that it does not sell data and deceived its Publisher and Advertiser clients by falsely claiming that all consumer identifying information was collected on an opt-in basis. In fact, Defendant does monetize and sell consumer data, much of which was collected using consent farms and therefore is not opted-in. Failing to disclose these practices constitutes false statements and/or material omissions of fact. If she had known Defendant was intercepting her communications and would monetize such communications, Plaintiff would not have signed up for or opened the email newsletter containing ads powered by LiveIntent.

145. Defendant's practices violate the unlawful prong of the UCL based on violations of privacy and consumer protection laws and the unfair prong of the UCL due to its deceptive statements and material omissions of fact.

146. As a result, Plaintiff and Class Members suffered a loss of property in the form of diminished privacy and loss of control over their personal data.

147. Plaintiff seeks restitution and injunctive relief pursuant to Cal. Bus. & Prof. Code § 17203.

COUNT VII

Violation of the Right to Privacy (Under the California Constitution) On Behalf of Plaintiff and All Class Members

148. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

149. The California Constitution, Article I, § 1, guarantees a fundamental right to privacy, which includes the right to control personal data and the right to be free from undue government and corporate intrusion into private life.

150. Defendant's conduct, including the unlawful collection, use, and sale of Plaintiff's personal data without notice or consent, including through deploying the LiveIntent tracking pixels, Defendant's RTB auctions, intent signal creation, and dossier-building and data disclosure, distribution, and resale, constitutes an invasion of Plaintiff's right to privacy as guaranteed by the California Constitution.

151. Defendants' actions were performed without adequate notice, consent, or authorization, in violation of Plaintiff's constitutional right to privacy.

152. Defendants' activities, including but not limited to their unconsented tracking, dossier-building, purchasing-intent inferring, and redistribution of such information, as described in this Complaint, are highly offensive and objectionable to the reasonable person.

153. As a direct and proximate result of Defendant's violation of Plaintiff's privacy rights, Plaintiff has suffered harm, including the loss of privacy, increased risk of data misuse, and exposure to harm arising from the improper collection and sale of her personal data.

154. Plaintiff seeks damages and injunctive relief to halt Defendant's ongoing violation of Plaintiff's privacy rights and to restore privacy protections.

COUNT VIII

Intrusion Upon Seclusion and Public Disclosure of Private Facts (Under California Common Law) On Behalf of Plaintiff and All Class Members

155. Plaintiff incorporates the preceding paragraphs as though fully set forth herein.

156. Defendant has intentionally, recklessly, and/or negligently interfered with Plaintiff's privacy by unlawfully collecting, storing, and sharing her personal information without her informed consent.

157. Under California common law, an individual has the right to control and protect their private information. Defendant's actions, including deploying the LiveIntent tracking pixel, Defendants' RTB auctions, intent signal creation, and dossier-building and data disclosure, distribution, and resale, were a direct invasion of Plaintiff's right to privacy and resulted in Plaintiff being deprived of her ability to protect her personal data.

158. Defendants' activities, including but not limited to their unconsented tracking, dossier-building, purchasing-intent inferring, and redistribution of such information, as described in this Complaint, are highly offensive and objectionable to the reasonable person.

159. On information and belief, the RTB auctions operated by LiveIntent and Zeta containing Plaintiffs' data constitute publication of private facts because they are easily accessed by anyone who seeks entrance with no legitimate gating function. All auction participants receive such data, not only bid-winners.

160. As a direct and proximate result of Defendant's actions, Plaintiff has suffered harm, including, but not limited to: loss of control over her private data, potential misuse of her personal information, and emotional distress.

161. Plaintiff seeks compensatory damages, punitive damages, and injunctive relief to remedy Defendant's violation of her privacy.

COUNT IX

Violation of New York General Business Law, § 349 and § 350 On Behalf of Plaintiff and All Class Members

162. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

163. Defendant has engaged in (1) consumer-oriented conduct, that is (2) materially misleading, and that (3) the plaintiff suffered injury as a result of the deceptive act or practice.

164. Defendant engaged in consumer-oriented conduct that was deceptive or misleading in a material way by failing to obtain informed consent from consumers before collecting their data using the LiveIntent tracking pixel and by failing to disclose its data harvesting practices and misrepresenting its privacy protections, including by falsely stating that it does not sell data and that it does not employ content farms to obtain identity data.

165. Plaintiff suffered actual harm as a result of Defendant's deceptive conduct, including loss of control over personal data and increased exposure to unconsented targeting, surveillance, tracking, identity profiling, and inference-gathering.

166. Defendant's practices include making material misrepresentations and omissions about the privacy and security of consumer data. Specifically, Defendant has falsely advertised the level of privacy and data protection it provides to consumers, despite unlawfully collecting, using, and selling personal data without adequate disclosure or consent.

167. Defendant deceived consumers by falsely claiming it does not sell data and deceived clients by falsely claiming that all identifying information was collected on an opt-in basis. In fact, Defendant does monetize and sell consumer data, much of which was collected using consent forms and therefore is not opted-in. Failing to disclose these practices constitutes false statements and/or material omissions of fact. If she had known Defendant was intercepting her communications and would monetize such communications, Plaintiff would not have signed up for or opened the email newsletter containing ads powered by LiveIntent.

168. Defendant's deceptive practices, including the disclosure, sale, and sharing of personal data without consent, constitute false advertising under New York General Business Law § 350.

169. Plaintiff and others similarly situated have suffered harm as a result of Defendants' false advertising, including loss of privacy and the inability to make informed choices regarding their personal data.

170. Plaintiff seeks actual damages, statutory damages, and injunctive relief to prevent further false advertising and to ensure that Defendant fully discloses its data practices.

COUNT X

Unjust Enrichment (Under California and New York Common Law) On behalf of Plaintiff and All Class Members

171. Plaintiff incorporates the preceding paragraphs as though fully set forth herein.

172. Zeta has wrongfully and unlawfully trafficked in Plaintiff's and the Class Members' PII without their consent and for substantial profits.

173. Plaintiff's and the Class Members' personal information is of monetary value to them and others.

174. Plaintiff's and the Class Members' personal information can be sold in legitimate and illegitimate markets.

175. Plaintiff held her personal information as an asset and sought to retain her ability to monetize her personal information if she wished to exchange it for monetary value at a later date.

176. Defendants obtained Plaintiff's and the Class Members' personal information without informed consent and fair exchange of economic value.

177. Plaintiff's and the Class Members' personal information and data have conferred an economic benefit on Zeta. For example, Zeta has unlawfully intercepted and used the Class Members' personal data to build cradle-to-grave dossiers on their habits and infer invasive intent signals for resale, all without informed consent or notice.

178. Defendant has been unjustly enriched at the expense of Plaintiff and Class Members, and has unjustly retained the benefits of its unlawful and wrongful conduct.

179. It would be inequitable and unjust for Zeta to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

180. Plaintiff and the Class Members accordingly are entitled to equitable relief, including restitution and disgorgement of all revenues, earnings, and profits Defendants obtained as a result of its unlawful and wrongful conduct.

181. Defendant has unjustly profited from tracking and disclosing to third parties Plaintiff's and Class Members' internet activity and real-world activity without Plaintiff's and Class Members' knowledge or consent. Plaintiff did not provide authorization for the use of her personal information, nor did Zeta provide her with control over its use to produce revenue. This unauthorized use of her information for profit entitles Plaintiff to profits unjustly earned.

182. It would be unjust and inequitable to allow Defendants to profit from their violation of Plaintiff's and the Class Members' constitutional, common law, and statutory rights as described herein.

183. Zeta was aware of the benefit conferred by Plaintiff. Indeed, Zeta's data marketplace and profit is premised entirely on selling and redistributing such data to third parties, regardless of how Zeta attempts to obfuscate, repackage, or rebrand the fact that it sells such data. Zeta acted in conscious disregard of the rights of Plaintiff and Class Members and should be required to disgorge all profit obtained therefrom to deter Defendant and others from committing the same unlawful actions again.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) For an order certifying the putative Class, naming Plaintiff as the representative of the putative Class, and naming Plaintiff's attorneys as Class Counsel to represent the putative Class Members;
- (b) For an order declaring that the Defendant's conduct violates the statutes referenced herein;
- (c) For an order finding in favor of Plaintiff and the putative Class on all counts asserted herein;
- (d) For statutory damages in amounts to be determined by the Court and/or jury;
- (e) For an order of restitution under California UCL for any funds improperly obtained through unlawful data collection or sales;
- (f) For prejudgment interest on all amounts awarded;
- (g) For an injunction restraining Defendant from continuing its unlawful data practices without informed consent, or, as the Court may deem proper;

- (h) For an order awarding Plaintiff and the putative Class their reasonable attorneys' fees, expenses, and costs of suit; and
- (i) For any other relief the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, demands a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: July 14, 2025

Respectfully submitted,

/s/ Gary E. Mason

Gary E. Mason (N.Y.S. Bar No. 2163467)

Danielle L. Perry*

Reuben A. Aguirre*

MASON LLP

5335 Wisconsin Avenue, NW, Suite 640

Washington, DC 20015

Tel: (202) 429-2290

Email: gmason@masonllp.com

Email: dperry@masonllp.com

Email: raguirre@masonllp.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice or applications for admission to be filed*